This project demonstrates a cryptographic toolkit implemented in Python, offering the following functionality:

1.Data Confidentiality (Symmetric Encryption)

2. Data Confidentiality (Hybrid Encryption)

3. Message Authentication assurance

prompting users to choose the cryptographic operation to perform.

Tutorial to run the code:

1) Make sure you have Python installed along with the required libraries.
2) Install the libraries needed to run the code from the CMD using the following commands:

   pip install pycryptodome

   pip install cryptography

   (make sure that the "pip" for python is installed in your device and is put in the same path)

3) After installing them, save the script with the (.py) extension, and run the code on the code-editor you choose (we used vs-code)

   4) the first operation is the symmetric key encryption, choose the No. 1 , then proceed to choose between encryption and decryption, in encryption insert your plain text and key, then choose one of the chaining modes, in decryption insert the cipher text with the key that encrypted it then choose between the 4 modes (ECB,CBC,OFB,CFB) to encrypt with.

5) For the second Operation, which is the hybrid encryption (digital envelope), choose No. 2, then choose between 3 modes, the first is the key generator, that generates an asymmetric key pair of the receivers side to use while encrypting and decrypting a message, the second is the encryption, insert your plain text then the public key generated above (just copy the public key file name given to you) and the encrypted data will be generated(encrypted key, cipher, and nonce), the last option is the decryption, you will be asked to give the encrypted key, then the nonce, the cipher text , and the private key, then the plain text will be shown and the decryption will end.
6) The last operation is the Message Authentication code, choose No. 3 in the toolkit, then choose between two choices, the first is the MAC Generator, to generate a Mac just enter the message and automatically you will be given the Message concatenated with the MAC and the timestamp, the second option is to verify a MAC, just write the input in the following format (message|timestamp|MAC code) without spaces, just this symbol " **|** " and will verify and tell if there is an error or if the message is Valid.

   That is the whole tutorial, Thank you for your patience, Have a Great Day !